Mitigating Security Threats in Tactical Networks

David Kidston, Li Li,
Communications Research Centre (CRC)
Ottawa, Ontario, Canada

{david.kidston, li.li}@crc.gc.ca

Helen Tang, and Peter Mason
Defence R&D Canada (DRDC)
Ottawa, Ontario, Canada

{helen.tang, peter.mason}@drdc-rddc.gc.ca

ABSTRACT

The future of tactical networks encompasses multi-hop digitised voice and data communications using VHF/UHF-band radios. While this radio band has excellent propagation properties, their relatively low bandwidth, high error rates and node mobility makes tactical radios less than ideal as a robust networking platform. Since networking is new to tactical communications, the security implications are not fully understood. Significant related research has been done for the network threats and vulnerabilities of commercial mobile ad-hoc networks (MANETs), however the threats in the literature are not always directly analogous because of the different communications characteristics. This paper takes a novel approach by reviewing known MANET security threats and then evaluating their potential impact on tactical networks. Though this analysis does not cover all possible security threats, it does leverage previous work and identify the most critical areas for further research. Based on this analysis, we propose the use of a cross-layer service framework to integrate security functions across all communication layers. A description of the framework and its application to several security areas are included.

1.0 INTRODUCTION

Tactical communications networks are limited by low bandwidth, high error rates and mobility. Existing protocols suffer degraded operations in the tactical environment to the point that very little useful operational information can be communicated, especially considering the additional bandwidth required for security. While there has been significant work in providing security for commercial mobile ad-hoc networks (MANETs) based on WiFi (IEEE 802.11 standards) [1,2], the security risks inherent in tactical networks are relatively unexplored in the open literature [3,4]. The critical differences between the two types of network are straightforward to enumerate.

- Tactical radios operate in the military VHF/UHF bands and provide bandwidth up to a hundred kbps. Tactical radios also typically provide jamming resistance (e.g., by using channel frequency hopping). WiFi based radios offer a data bandwidth in the Mbps.
- Tactical radios support robust long range signals of 5 to 30 km through complex terrains [5].WiFi networks have limited range, up to several hundred meters under ideal conditions.
- Tactical mobility is also quite different from mobility assumed in the commercial environment. Tactical networks are directed instead of random, leading to a more coherent (grouped) movement pattern where nodes will be more concentrated instead of moving between random waypoints.
- Due to the short range of WiFi networks, information security is based on encryption while tactical networks must deal with muti-level security and strong authentication concerns.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
SEP 2010	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Mitigating Security Threats in Tactical Networks	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Communications Research Centre (CRC) Ottawa, Ontario, Canada**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADA568727. Military Communications and Networks (Communications et reseaux militaires). RTO-MP-IST-092

14. ABSTRACT
The future of tactical networks encompasses multi-hop digitised voice and data communications using VHF/UHF-band radios. While this radio band has excellent propagation properties, their relatively low bandwidth, high error rates and node mobility makes tactical radios less than ideal as a robust networking platform. Since networking is new to tactical communications, the security implications are not fully understood. Significant related research has been done for the network threats and vulnerabilities of commercial mobile ad-hoc networks (MANETs), however the threats in the literature are not always directly analogous because of the different communications characteristics. This paper takes a novel approach by reviewing known MANET security threats and then evaluating their potential impact on tactical networks. Though this analysis does not cover all possible security threats, it does leverage previous work and identify the most critical areas for further research. Based on this analysis, we propose the use of a cross-layer service framework to integrate security functions across all communication layers. A description of the framework and its application to several security areas are included.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**26**	

- Tactical networks use TDMA for guaranteed QoS and to ensure MLPP. WiFi networks use a contention based MAC scheme, which provides fair access to the wireless medium.
- Finally, unique to tactical networks, nodes are preconfigured with set addresses and cryptographic keys for bootstrapping security. However, there is still a need for on-line key revocation and updating.

While the vulnerabilities of MANETs and tactical networks are similar, the threats and impacts are different. We have leveraged the research on MANET threats and analysed their impact on tactical networks. In this paper we explore the impact of tactical network characteristics on network security through two pieces of foundational work. First we take a closer look at the risk of MANET security threats specifically to tactical networks in a bid to better understand their security requirements. Second, we propose a framework to help improve security in this environment by dealing with the particular characteristics of tactical networks.

One typical solution for dealing with wireless network characteristics is to find cross-layer efficiencies by sharing information between protocol layers. Each layer can then optimise its performance based on a more complete picture of the state of communications locally and potentially within the rest of the network. There has been significant research in the use of this cross-layer design in MANETs. Indeed, John Stine proposes in [6] that cross layering is a requirement for efficient MANET design and operation since the current layered design prevents desirable interactions between layers that can be exploited for improved performance. For this reason, we propose the use of a cross layer framework to improve efficiency and coordinate security in tactical networks.

This paper continues in Section 2 with a threat classification system based on MANET security research. Using this classification, Section 3 provides a high level risk analysis of the identified threats in tactical networks and some controls (possible solutions) from the MANET literature are identified. Section 4 provides a description of the cross-layer framework. In Section 5 the potential impact of the cross-layer framework on three security services is discussed. Section 6 provides a more in depth investigation of the framework through a case study before the paper concludes in Section 7.

2.0 THREAT CLASSIFICATION

The key to information protection is maintenance of confidentiality, integrity and availability (CIA). Over time, a number of attacks on networks have been devised each attempting to compromise one or more of the CIA principles. These attacks can be grouped into different types of threats [7]. We consider two main types of threats for tactical networks. Passive threats are based on an attacker who does not emit energy while observing the energy transmitted from other sources. Active threats are based on an attacker who actively transmits energy.

2.1 Passive Threats

Two types of passive threats are considered here. While traffic analysis is of more critical to tactical networks security, both types of network are sensitive to eavesdropping.

Traffic Analysis: Involves an adversary who collects transmitted energy, traffic flows (protocol headers), sizes, and/or timings to gather insight into the network topology and traffic patterns. This is a serious threat in tactical networks due to their small size, wireless bandwidth and long range. Though message contents cannot be read, the relative importance of nodes and tempo of operation can be determined. Tactical networks are quite vulnerable to this threat as it is straightforward to accomplish with limited knowledge of the network being observed.

Eavesdropping: Involves an adversary who examines the content of messages to gather the information transmitted. Again tactical networks are at risk. In this case, the threat is to confidentiality. Tactical networks have a relatively low vulnerability to this threat due to the many layers of security that must be penetrated (up to the application level), but the loss of information privacy could have a significant impact.

2.2 Active Threats

For active threats the adversary transmits at the frequency used by the tactical network. This makes it more dangerous for the adversary as it leaves them open to counter measures (which are not discussed here).

Denial of Service: Involves an adversary who uses the transmission of packets or raw energy to deny or delay service to authorized participants. There is a wide spectrum of threats, basically one per network layer. At the physical layer, jamming raises the noise floor to the point that nodes in the vicinity cannot decode network traffic [8]. At the network layer the routing protocol might be compromised invalidating packet forwarding or spurious packets can be used to overload the available bandwidth (e.g. gray-hole and rushing [9]). All networks are vulnerable to and impacted by the loss of availability inherent in physical layer attacks. Attacks higher in the protocol stack are made difficult due to the multiple layers of security services.

Masquerade: Involves an adversary who emulates or acquires one or more valid nodes within a network in order to perform an attack (e.g. wormhole and sybil [2]). This threat is relatively unlikely in tactical networks where the possibility of creating or capturing (and then successfully using) a compatible platform is limited. There is however a significant impact on confidentiality and integrity if such an attack were successful as critical information transmitted could be collected, and potentially modified (see below).

Modification: Involves an adversary who alters the content (e.g. node exposure and route manipulation [9]) of an intercepted message and then passes it on. The adversary must be an authenticated member of the network in order to accomplish this. A masquerading node is capable of modification up to and including at the application level. Due to the multiple levels of security at each layer, tactical networks are unlikely to be compromised at a high enough level to interfere with the confidentiality and integrity of the network. Compromised availability is the mostly likely result of this type of threat.

3.0 QUALITATIVE RISK ANALYSIS

Based on the threats described in the previous section, some preliminary analysis can be made about their impact based on which layer has been compromised. For our qualitative analysis, we determined risk based on the vulnerability of tactical networks to a threat (the weakness or lack of available controls that would allow or facilitate the threat), and impact of a threat (the value of the asset being attacked, related to the adverse affects if the attack were successful). Our analysis is focused primarily on the network and its ability to transfer information based on the CIA principles.

At the physical layer, a compromise requires knowledge of the physical medium being used (e.g. frequency for jamming or traffic analysis). The impact of jamming is serious, impacting availability (of information in the area jammed, and potential network wide if the network is partitioned). The impact for traffic analysis is a loss of confidentiality (e.g. of network topology).

At the MAC layer, a compromise requires knowledge of the protocols that negotiate access to the physical medium (e.g. hello signal for node exposure). Since tactical networks typically use TDMA as opposed to 802.11 based protocols the risks are different from MANETs. While node exposure (loss of confidentially) and replay attacks (loss of availability) are not significantly different in tactical networks, the nature of the MAC make them less of a vulnerability (see frequency hopping below).

At the network layer, a compromise requires knowledge/participation in the routing mechanism used (e.g. route building sequence for black-hole). Since the physical and MAC layers must be compromised first, there is less of a threat. Non-cooperative nodes such as grey hole nodes effect the availability of information by interfering with traffic forwarding (a denial of service). Traffic analysis at the network layer impacts the confidentiality of all information that comes within range of the adversary. Finally route manipulation (modification) has a significant impact as this can deny communications across the entire network.

For higher layers, a compromise requires knowledge of the communicating applications (e.g. application layer formatting for traffic snooping) as well as compromising all lower layers. The impact of such attacks can be significant. Both flooding and sleep deprivation affect the availability of the attacked node as well as the intervening network. Snooping at the application layer should be noted for its impact as it is the only attack that affects the integrity of the message. If the attacker can read and modify packets in transit (masquerade) information security has been completely compromised.

An exact calculation of the impact of each of the attacks depends on the circumstances under which the attack was attempted and there is material available in this area for further research. Attacks at higher layers require greater expertise, deeper access into the network, and a greater outlay of resources compared to the attacks possible at lower layers. For tactical networks where access is limited due to mobility and rapid deployment and tear down, outsider attacks at the lower layers that require little knowledge are more likely though they have less impact in terms of information security. A summary is presented in Table 1.

Table 1: Qualitative Risk Analysis for Tactical Networks

Threat	***Vulnerability***	***Impact***	***Risk***	***Primary Control***
Denial of Service	Low-High	High	Low-High	Layer specific mechanisms [1]
Eavesdrop	Low	High	Low	Cryptography [10]
Masquerade	Low	Very High	Medium	Trust System [11] and Cryptography
Modification	Low	High	Low	Cryptography
Traffic Analysis	High	Low	Medium	Traffic Obfuscation [12]

Denial of service has a variable risk depending on the level at which the attack is made. At the physical level the risk can be considered high (even for MANETs) since there are limited controls. Frequency hopping in tactical networks mitigates this to some extent, as can power control [13].Eavesdropping has a low risk due to the low likelihood of gaining access to the application layer. The use of authentication and encryption at the higher protocol layers ensures information integrity while at lower layers can reduce or eliminate external attacker based vulnerabilities. Masquerade is also unlikely, but since nodes may be captured for this purpose, the risk may be considered medium. Besides cryptography, a trust system can add additional control where the suspicions of multiple nodes are combined, making better attack detection possible. Similarly packet and traffic modification at levels below the application level are unlikely due to cryptography giving low risk. Finally traffic analysis is of high vulnerability at the

physical layer though it has a lesser impact. Little can be done to detect this type of attack, but traffic obfuscation, where the number and size of messages are changed by splitting and merging packets onto different routes, can make traffic analysis less valuable.

4.0 CROSS-LAYER SECURITY FRAMEWORK

Cross-layer design has been proposed for a number of reasons in the past. It has been argued that it provides an **efficient** solution through information sharing and coordination between layers [6]. This allows security services at the upper layer, such as authentication and intrusion detection to use information from secure sensing at Layer 1 (physical) and Layer 2 (data link) to improve operations. Security services are needed at different layers for different functions. The basic security functions including authentication and intrusion detection can be integrated as cross-layer security services and the results can be used by different communication layers. While this framework may increase some of the internal processing within a node, it can reduce the communication between nodes. This is critical to tactical networks where communication is the most expensive resource. Cross-layer design can also **coordinate** operations, improving response time and reducing the possibility of security mechanisms in specific layers working at cross-purposes to one another. For example, if jamming is detected a coordinated response might be for the physical layer to increase transmission power, the MAC layer to increase error correction coding and the application layer to notify the user of an attack currently underway and ask for help in determining an appropriate response. Without such coordination the MAC layer might increase retransmissions and the network layer begin a new round of routing queries, exacerbating congestion and further denying service in the area being jammed.

4.1 Proposed Framework

Our approach focuses on a cross-layer solution suited for security and management functions for tactical networks at all protocol layers. We have proposed the use of a publish-subscribe system as a vertical interface between the protocol layers [14]. This can be used as a messaging system available to all layers so that critical real-time operational metrics can be shared as desired. For this reason we called this messaging system the Metric Store. Each protocol layer that has been enhanced with access to the Metric Store is able to publish their internally calculated and derived operational metrics. These metrics can be subscribed to by any other enhanced layer or by an independent cross-layer service. Cross-layer services such as network security are concerned not with the operation of any particular layer, but can be considered as system services that provide additional guidance/metrics to be used by any interested enhanced layer. The complete architecture is shown in Figure 1.

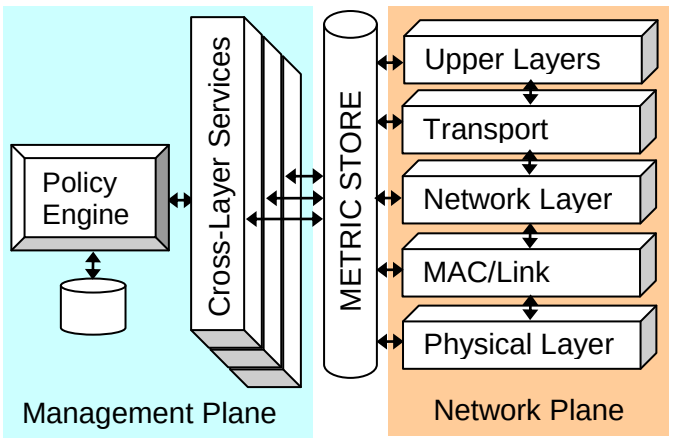


Figure 1: Cross Layer Architecture.

Besides the network store, the protocol layers (including security interfaces between layers) can be enhanced to make use of information shared through the Metric Store. This information may be published by other layers or cross-layer services. Interoperability with un-enhanced layers is ensured since the standardised horizontal interface between layers remains unchanged. Enhanced layers will continue to operate even if cross-layer information they would like to use is not available. Care must be taken to ensure that protocol layers on each node remain consistent in the case where the node will need to communicate with remote nodes that are not cross-layer enhanced. Similarly, note that if a layer is not enhanced it will still be able to perform its normal function. Though it will not participate in cross-layer optimisations, the complete network stack will continue to operate correctly.

This architecture was designed to coordinate protocol operations (including security) across the various communication layers. Unlike previous recommendations for cross layer design, we consider the development of separate cross-layer services for the purpose of protocol stack wide enhancements such as network management and security. These services interact with the Metric Store in the same way as enhanced protocol layers. They have access to the complete set of metrics from all layers and at the same time are unburdened by layer-specific requirements. Each protocol layers can thus focus on their core functionality while subscribing to value-added metrics instead of calculating them locally. For example, per-layer information can be combined to build a security situational awareness picture that can aid the operator or an automated management system to determine an appropriate course of action to a network attack. This type of design can also mitigate the effect of individual security mechanisms operating at different protocol layers from working at cross-purposes to one another.

In order to aid in the operation of the cross-layer service, a mechanism for directed automation and adaptation has been added to our architecture. Policy-based systems are well known for their support of network management functions, and can also be of use for directing other services such as security. In tactical networks coordination among nodes may be limited by bandwidth constraints. For this reason the use of policy directives (which are generally less resource intensive than configuration scripts) are desirable for tactical networks.

4.2 Previous Work

There has been significant work in cross-layer optimisation for WiFi-based wireless networking [15], but relatively little in terms of tactical networks. One exception is [16] in which an architecture that proposes the use of a vertical management plane to coordinate the layers (similar to cross-layer services), but without a commonly accessible data store. This requires all cross-layer data to pass through a single controller so that only a single monolithic cross-layer service is possible (no independent per-layer enhancements). This research, like much in the field, focuses specifically on QoS requirements and little on other network management activities in the network. Another exception is [17] where Policy-based management (constraint satisfaction) is applied universally to solving problems in routing, network planning, mission planning and spectrum allocation for tactical networks. Our work is less all encompassing and focuses on an adaptive management solution which is suited for all communication layers.

Another interesting area of cross-layer related research is found in [18] where nodes with at least two radios speed up end to end transmission of critical traffic by re-transmitting packets on one channel as they are being received on the other. This requires end-to-end reservations on the channels affected with interactions between physical, MAC, and network layers.

Significant work in cross-layer network design was completed in the MobileMAN project [19]. This research has a similar architecture including a vertical inter-layer message system. Again QoS is the focus of the work with a modified routing algorithm used to pass p2p service identifiers to all nodes in a system on top of existing routing transmissions. Though interesting, this is an example of a backchannel method

of passing application information, not the kind of cross-layer based communication and security optimisations that we are pursuing in this work.

5.0 CROSS-LAYER SECURITY SERVICES

There are advantages to using this cross-layer architecture for security in tactical networks. By taking metrics from the security services at one layer, such as from authentication systems and intrusion detection systems (IDS), operations at other layers can be made more secure or optimised. For example, authentication and intrusion detection systems operating at the application layer can provide real-time attack profiles into an integrated cross-layer security service. The results (metric or metrics) can then be used by the lower layers to improve their efficiency (they don't have to calculate the security metric themselves) and robustness (security is derived from the multiple methods used across the various communication layers). While this framework may increase the complexity and internal processing within a node (in order to integrate multiple functions), it should reduce the communication requirements between nodes (since confirmation with neighbouring nodes is no longer as critical). This is especially beneficial to tactical networks where bandwidth is limited. Some potential security services that could be integrated using this framework are described below.

5.1 Intrusion Detection

Intrusion detection systems (IDS) are employed to determine when the network is being subjected to a network or application layer attack. Such systems are one of the more effective ways to counter, for example, masquerade threats [20]. An IDS can benefit from the establishment of a "trust model", for example, to distinguish among friends, acquaintances and adversaries. An intrusion detection or similar behavioural analysis engine can be charged with monitoring neighbours. In tactical networks, the IDS will likely need to be distributed rather than centralised. This leads to a "watchdog" approach where nodes monitor and analyse the behaviour of their local neighbours.

Lessons can be drawn from existing work in the area of Byzantine routing, including consensus algorithms to eliminate falsified information, which can make the system more robust. There are also various methods of establishing trusted routes based on hash chains and digital signatures, but these methods may prove to have too much overhead and consume too much bandwidth to be applicable to tactical networks [21]. In fact, many of the security overlays proposed in the area of ad hoc networking suffer from overhead issues or complicate the communication protocols such that interoperability among coalition partners could be threatened if different security solutions are employed. Research is being conducted that allows for the provision of security services such as intrusion detection and authentication in mobile ad hoc networks without relying on additional messaging [18], however it is often the case that detection of an attack at one layer requires mitigation techniques be applied at another. For example, if a Sybil attack), in which a node claims several identities (Masquerade), is detected at the application layer, the response may be to block all traffic coming from the attack's location by eliminating the route from the routing table [22].

5.2 Frequency Hopping

Frequency hopping is a well known physical layer defence against frequency jamming. The radio transmits on a set of frequencies in a pre-determined sequence followed by all corresponding nodes in the tactical network. By using frequency hopping, a wider range of the spectrum is used making it more difficult for an adversary to transmit sufficient energy within that band to interrupt the demodulation at the receiver.

One of the potential benefits of cross-layer enabling the physical layer is the use of application level characteristics to understand when and to what extent jamming is expected to be a problem. In a time of transmission of critical information, or when the node is in a physical location known to be prone to jamming, the rate and range of frequency hopping can be tuned to the application level requirements based on a security policy. That is, application layer analysis can be used to dynamically modify physical layer attributes.

5.3 Distributed Authentication

For security services in a distributed network, threshold cryptography is generally used to let some or all network nodes share a network master key and collaboratively provide security services such as issuing and refreshing private keys. In a network with N nodes, a group of n special nodes is capable of generating partial certificates using their shares of the certificate signing key. A valid certificate can be obtained by combining k such partial certificates, which is called (k, n)-threshold cryptography.

In MANETs, identity (ID)-based cryptography with threshold cryptography is a popular approach for the security design because key management is simpler than that of public key infrastructure (PKI). In threshold schemes, the network can tolerate the compromise of up to (k −1) shareholders. The security of the whole network is breached when a threshold number of shareholders (k) are compromised. Therefore, the optimal selection of nodes in threshold cryptography should be carefully investigated. However, most previous work for key management in this framework concentrates on the protocols and structures. Consequently, how to optimally conduct node selection in ID-based cryptography with threshold secret sharing is largely ignored. In [23], a distributed scheme based on the stochastic multi-arm bandit formulation is proposed. The proposed scheme can select the best nodes for reconstructing the full secret taking into account the security conditions to minimise the overall threat posed to the network. We can utilize the information obtained from the Metric Store for node selection. For example, we can assign a weight value for a node based on the information from Metric Store. If a node has high security, it may have higher weight. We then conduct the node selection process considering the weights to achieve higher security.

6.0 CASE STUDY: LIGHTWEIGHT INTEGRATED AUTHENTICATION

In order to further validate our architecture, this section describes a security problem for tactical networks and details how a solution can be augmented using our cross-layer architecture. We base the case study on previous work on the lightweight integrated authentication (LIA) scheme in MANETs [24]. Authentication is an important element of network security because it is the first step toward prevention of, and guarding against, unauthorized access to network resources and sensitive information. We hope to efficiently utilize the authentication results for other security services such as secure routing through the cross-layer scheme. LIA is summarised below, followed by a discussion of how it could be adapted to and benefit from a cross-layer design such as the one detailed in this paper.

6.1 Overview of LIA

In the LIA scheme, each node maintains a trust table which is a fusion of security information of all the neighbouring network nodes. It is first established based on authentication and then kept updated based on any available intrusion detection systems (IDSs) and the key self-revocation mechanism of LIA. The value of the trust field can be thought of as raw data – its utilisation is application dependent [22].

The details of managing the trust table are provided as follows:

Step 1: Bootstrapping: As described by McGrath et. al. [25], LIA uses an off-line PKG that generates Identity Based Encryption (IBE) private keys for all devices based on their unique identities. This is feasible in tactical networks because before deployment, users with their devices have to report to a command post where the Private Key Generator (PKG) could be located.

Step 2: Pre-authentication: Using its private key and the public key of its recipient node, every node can compute its pairwise symmetric key for authentication with the recipient. This key is the same for both nodes because of the bilinearity property of IBE [26].

Step 3: Credential establishment: A pairwise symmetric key is communicated between the two nodes. The symmetric key is encrypted for confidentiality using the public key of the recipient, and signed for authentication using the private key of the sender.

Step 4: Authentication: Mutual authentication is performed when the two nodes compare their pair-wise symmetric keys. This key can also be used as session key for securing the data communications. A trust table is then built to store the trust values of its neighbours. The value of the trust field can be either Boolean (e.g., zero or one) or multi-level (e.g., zero, low, medium, high). Once node i is authenticated by node j, the trust value of node i can be set to one in node j's Trust Table. When the public key of node i is revoked, the trust value of node i can be set to zero in node j's Trust Table. The Trusted routes could then be established through authenticated nodes with non-zero trust values. Security policy can define if a message can be routed through all available routes or only trusted routes

Step 5: Monitoring: This is accomplished through continuous user-to-device authentication with IDS. User and device are assumed to be tightly coupled in a tactical operation. When user-to-device authentication fails, it implies that the device is not in the hands of a legitimate user. This event triggers revocation of the public key of the device. We recommend performing user-to-device authentication through wearable biometric sensors because they have the following properties: 1) direct user binding, 2) non-disruptive re-authentication, 3) inherent liveliness detection [27].

Step 6: Revocation: LIA introduces a self-revocation mechanism by leveraging the integration of user-to-device and device-to-network authentication. This concept is illustrated in Figure 2. Once the user-to-device authentication fails, which implies the compromise of the device, the device informs the neighbouring nodes using a GoodBye message. The node will then be excluded from the trusted routes of its neighbors. The GoodBye message is similar to a Hello message in a proactive routing protocol such as the Optimised Link State Routing protocol (OLSR) [28] but it performs a GoodBye-type operation, excluding the sender from its neighbours' trusted routes. The existing message handlers in OLSR can be re-used to process this message to implement the Distributed Revocation Authority and to propagate the GoodBye message to neighbouring nodes' Trust Tables.

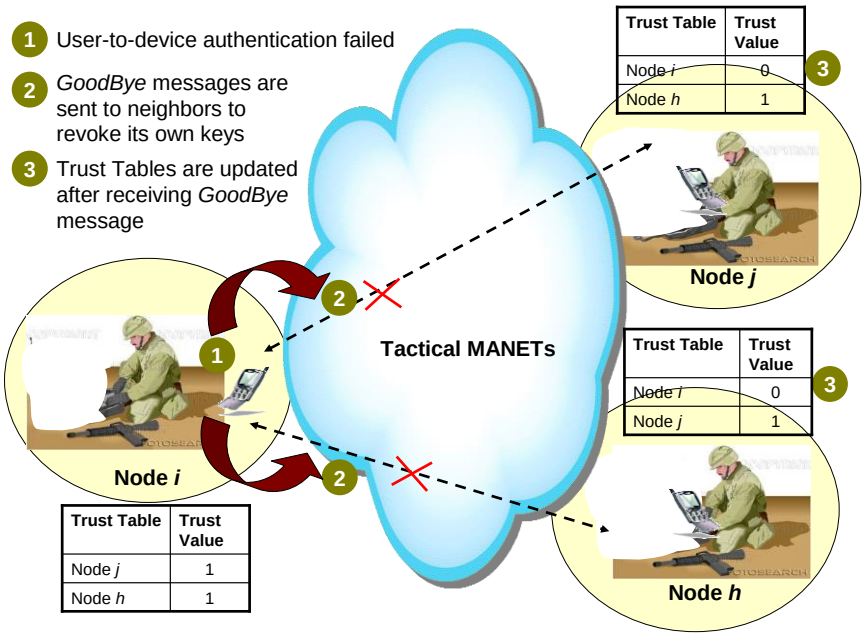


Figure 2: LIA's Self-revocation Mechanism.

In order to create a GoodBye message, LIA proposes adding a LinkType to the existing format of the Hello message indicating that the trust value of the sender should be changed to zero in the receivers' trusted routing table. The GoodBye messages must be encrypted and sent to all the neighbours as adversaries may fabricate such messages to cause public keys of uncompromised nodes to be revoked – a denial of service attack.

6.2 LIA within a Cross-layered Architecture

As mentioned in Section 5.1, the trust table can be viewed as the fusion of the security information of all network nodes. As such, it is a natural extension to allow the trust table to be a part of the Metric Store. The trust value can be set with the authentication and IDS results obtained in the application layer, results which can also be part of the Metric Store. Any layer that is interested in the trust values can subscribe to the service and access the trust table. In the following, we list 4 examples showing how 4 layers can enhance their security by utilizing the trust values.

1. At the session layer, a security policy can be defined to allow applications establish sessions with those nodes that have a minimum trust value. During a session establishment, in addition to session parameters such as IP address and port number, the trust value of a node is also communicated. The source node automatically decides whether to continue establishing a session to that destination node or not. The applications can range from e-mail, FTP, HTTP, VoIP or even a video or data session. Deploying this approach at session layer not only eliminate user intervention but also reduces the security risks while adaptively adjust to time varying security requirements.

2. At the routing layer, routing table can be built incorporating the trust values. The routing table is built based on certain routing algorithms such as OLSR [26]. The security of routing algorithms is usually addressed through cryptographic algorithms. If we could incorporate the trust values when we build the routing tables, we can more efficiently enforce certain security policies such as letting a message be routed through any available route or only through nodes with certain trust value. This feature is especially useful in coalition operations where multiple countries cooperate but with different security

requirements. For example, certain encrypted messages like command and control messages for designated receivers must be routed through nodes with a minimum trust value.

3. For MAC layer, longer medium access time may be allocated to the nodes that have higher trusted value;

4. For physical layer, we can utilize the information obtained from the trust table for distributed spectrum sensing. We can increase the trustworthiness of the spectrum sensing results by assigning higher weights to the sensing results obtained from nodes with higher trust values.

There are two main advantages of using LIA within this scheme for tactical MANETs. It results in less communication overhead between nodes and it enhances the security at different layers, allowing greater flexibility in defining the security policy according to application needs.

7.0 CONCLUTIONS AND FUTURE WORK

Tactical networks and MANETs have many similarities, including a wide variety of security threats that take advantage of wireless communications and ad-hoc routing mechanism. Tactical networks differ in their extremely low bandwidth, long range, low mobility and the ability to configure all nodes with set addresses and cryptographic keys in advance. Threats from existing MANET research have been evaluated in this paper in light of the particular characteristics of tactical networks.

This paper proposes the use of a cross-layer framework to help solve network security issues in tactical networks. The proposed framework supports automation and efficiency well suited to tactical networks. As illustrated in a number of examples, the framework may promote improved efficiency and coordination of security services across communication layers.

We are currently in the process of designing a cross-layer intrusion detection service which makes use of the proposed framework. We plan to use a simulation of tactical networks to gain quantitative measurements of the effectiveness of cross-layer controls compared to existing single layered controls.

8.0 ACKNOWLEDGEMENTS

This work was supported by Defence R&D Canada (DRDC).

9.0 REFERENCES

[1] B. Wu,et al. “A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks”, In Wireless/Mobile Network Security. Y. Xiao, X. Shen and D-Z. Du (eds), Springer, 2008.

[2] B. Kannhavong et al. “A survey of routing attacks in mobile ad hoc networks,” in IEEE Wireless Communications Magazine, Vol 14, No. 5, pp 85-91, Oct. 2007.

[3] J.L. Burbank et al, “Key Challenges of Military Tactical Networking and the Elusive Promise of MANET Technology”, IEEE Communications Magazine, Vol 44, No. 11, 2006, pp. 39-45.

[4] S. Jacobs, “Tactical Network Security”, proceedings of IEEE Military Communications Conference, vol. 1, pp. 651-655, Nov. 1999.

[5] J. Pugh, R. Bultitude, and P. Vigneron, “Propagation Measurements and Modelling for Multiband Communications on Tactical VHF Channels”, proceedings of IEEE Military Communications Conference, Oct. 2007.

[6] J.A. Stine, “Cross-Layer Design of MANETs: The Only Option”, in IEEE Military Communications Conference, 2006, pp. 1-7.

[7] A. Martin, J. Smith, and M. Koethe, “A Platform Independent Model and Threat Analysis for Mobile Ad hoc Networks”, proc. of the 2007 Software Defined Radio Technical Conference, Denver, Colorado, Nov. 2007.

[8] W. Xu, W. Trappe, Y. Zhang, and T. Wood. “The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks”., proceedings of the Sixth ACM International Symposium on Mobile Ad Hoc Networking and Computing, May 2005.

[9] I. Aad, J. Hubaux, and E. Knightly. “Denial of Service Resilience in Ad Hoc Networks,” proceedings of the Tenth Annual ACM Conference on Mobile Computing and Networking, Sep.-Oct. 2004.

[10] J. Chen and J. Wu, "A Survey on Cryptography Applied to Secure Mobile Ad Hoc Networks and Wireless Sensor Networks" to appear in Handbook of Research on Developments and Trends in WIreless Sensor Networks: From Principle to Practice, H. Jin and W. Jiang (eds), IGI Global, 2010.

[11] H. Wang, Y. Wang, J. Han, “A Security Architecture for Tactical Mobile Ad Hoc Networks”, Second International Workshop on Knowledge Discovery and Data Mining, 2009, pp. 312-315.

[12] D. Huang and V. Kandiah, “Low-Latency Mix Using Split and Merge Operations”, Journal of Network Systems Management, Vol. 18, Num. 3, 2010, pp. 244-264.

[13] T. Faha, D. Djenouri and R. Askwith, “On Detecting Packets Droppers in MANET: A Novel Low Cost Approach”, Third International Symposium on Information Assurance and Security, 2007, pp. 56-64.

[14] D. Kidston and L.Li, “Management through cross-layer design in mobile tactical networks”, IEEE Network Operations and Management Symposium (NOMS), 2010, pp. 890-893.

[15] X. Wang, J.S. Wong, F. Stanley and S. Basu, "Cross-Layer Based Anomaly Detection in Wireless Mesh Networks," IEEE/IPSJ International Symposium on Applications and the Internet, pp. 9-15, 2009

[16] S. Ci and J. Sonnenberg, “A Cognitive Cross-Layer Architecture for Next-Generation Tactical Networks", IEEE Military Communications Conference, 2007.

[17] G. Denker, et al., “An Architecture for Policy-Based Cognitive Tactical Networking” in IEEE Military Communications Conference, 2006, pp 1-7.

[18] L. Romdhani and C. Bonnet, “Achieving a good trade-off between complexity and enhancement in cross-layer architectures”, in Proceedings of the 2nd International Conference on Information and Communication Technologies, 2006, pp. 2473-2478.

[19] M. Conti, G. Maselli, and G. Turi, "A Flexible Cross-Layer Interface for Ad-Hoc Networks: Architectural Design and Implementation Issues" in Ad Hoc & Sensor Wireless Networks, Vol. 2, Num 2, 2006, pp. 398-415.

[20] D. Lynch et al., Providing Effective Security in Mobile Ad Hoc Networks Without Affecting Bandwidth or Interoperability, in Army Science Conference 08, 2008.

[21] Y.C. Hu and A. Perrig, A Survey of Secure Wireless Ad Hoc Routing, in IEEE Security and Privacy, 2004.

[22] F. R. Yu, H.Tang, F. Wang, V. C.M. Leung, Distributed Node Selection for Threshold Key Management with Intrusion Detection in Mobile Ad Hoc Networks, in the 2009 IEEE/IFIP International Symposium on Trusted Computing and Communications (TrustCom-09), Vancouver, Canada, August 29-31, 2009.

[23] John R. Douceur, The Sybil Attack, Revised Papers from the First International Workshop on Peer-to-Peer Systems, p.251-260, March 07-08, 2002

[24] H. Tang and M. Salmanian, Lightweight Integrated Authentication for Tactical MANETs, in International Symposium on Trusted Computing (TrustCom-08), Zhangjiajie, China, Nov. 18-21, 2008.

[25] C. McGrath, A.S. Ghazanfar and M. McLoone, Novel Authenticated Key Management Framework for Ad Hoc Network Security, in Proceedings of. ISSC 2006, Dublin, June, 2006.

[26] D. Boneh, and M. Franklin, Identity-based encryption from the Weil Pairing, in Advances in Cryptology – CRYPTO '2001, LNCS 2139, pp 213-229, 2001.

[27] H. Tang, M. Salmanian and Q. Xiao, Biometric-based User Authentication for Tactical Mobile ad-hoc networks, DRDC Ottawa Technical Note 2007-100, May 2007.

[28] T.Clausen and P.Jacquet, Optimized Link State Routing Protocol (OLSR), IETF RFC 3626, October 2003. http://www.ietf.org/rfc/rfc3626.txt

Mitigating Security Threats in Tactical Networks

David Kidston, Li Li,
Helen Tang, and Peter Mason

Communications Research Centre (CRC)
Defence R&D Canada - Ottawa

Overview

- Tactical Networks vs. MANETs
  - Similar, but different
- Wireless Security
  - Lots of work published on MANETs
  - Some lessons for risks to tactical networks
- Cross-Layer Framework
  - Potential efficiencies and coordination benefits
- Use Cases
  - How can cross-layer services be used to improve security in tactical networks?
- Conclusions

Tactical Networks vs. MANETs

- Tactical radios provide robust bandwidth up to one hundred kbps, and support robust long range signals of 5 to 30 km through complex terrains.
- Tactical networks are directed instead of random, leading to a more coherent (grouped) movement pattern where nodes will be more concentrated.
- Tactical networks must deal with muti-level security and strong authentication concerns.
- Tactical networks use TDMA for guaranteed QoS and to ensure MLPP.
- Nodes are preconfigured with set cryptographic keys.

- WiFi networks have limited range, up to several hundred meters under ideal conditions, and offer a data bandwidth in the Mbps.
- MANETs assume Random Waypoint or other symmetric mobility models
- Security is focused on information security (based on encryption)
- WiFi networks use a contention based MAC scheme, which provides fair access to the wireless medium.
- Assume no or little trusted key infrastructure.

MANET Threat Classifications

- Passive Threats
  - No emissions so harder to detect
- Traffic Analysis
  - Used to determine relative importance of time/location
  - All networks vulnerable, but impact relatively low.
- Eavesdropping
  - An attack on confidentiality
  - Fairly low vulnerability, but difficult to perform consistently in mobile environment.

MANET Threat Classifications (cont'd)

- Active Threats
  - Participate in the network so greater impact, but easier to detect
- Denial of Service
  - Jamming at physical layer particularly effective
  - More difficult at higher layers (black hole,
- Masquerade
  - Strong authentication required
- Traffic Modification
  - Similar to masquerade, but more technically challenging

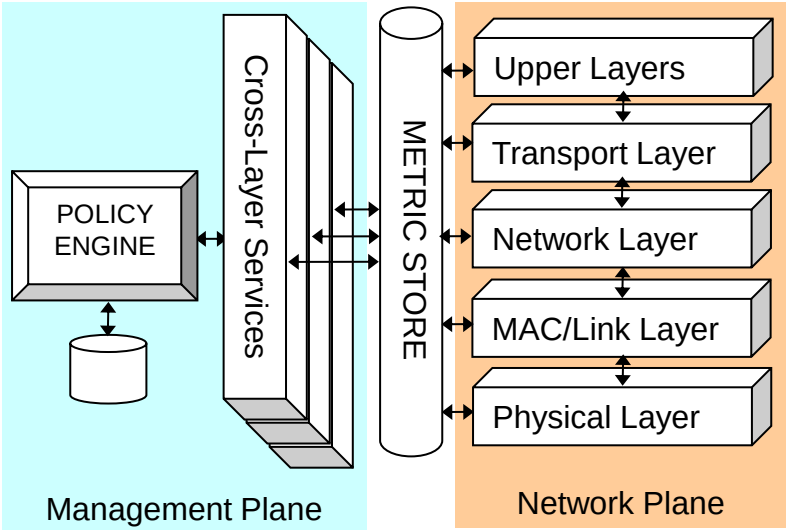
Risk Analysis

- Physical Layer requires knowledge of the physical medium being used
- MAC Layer requires knowledge of the protocols that negotiate access
- Network Layer requires participation in the routing mechanism
- Higher Layers requires knowledge of the application details

Threat	***Vulnerability***	***Impact***	***Risk***	***Primary Control***
Denial of Service	Low-High	High	Low-High	Layer specific mechanisms [1]
Eavesdrop	Low	High	Low	Cryptography [10]
Masquerade	Low	Very High	Medium	Trust System [11] and Cryptography
Modification	Low	High	Low	Cryptography
Traffic Analysis	High	Low	Medium	Traffic Obfuscation [12]

Cross-Layer Framework

- Metric Store (publish – subscribe)
- Per-layer enhancements (network plane)
- Cross-Layer Services (management plane)
- Policy Engine (automation)



Sample X-Layer Security Services

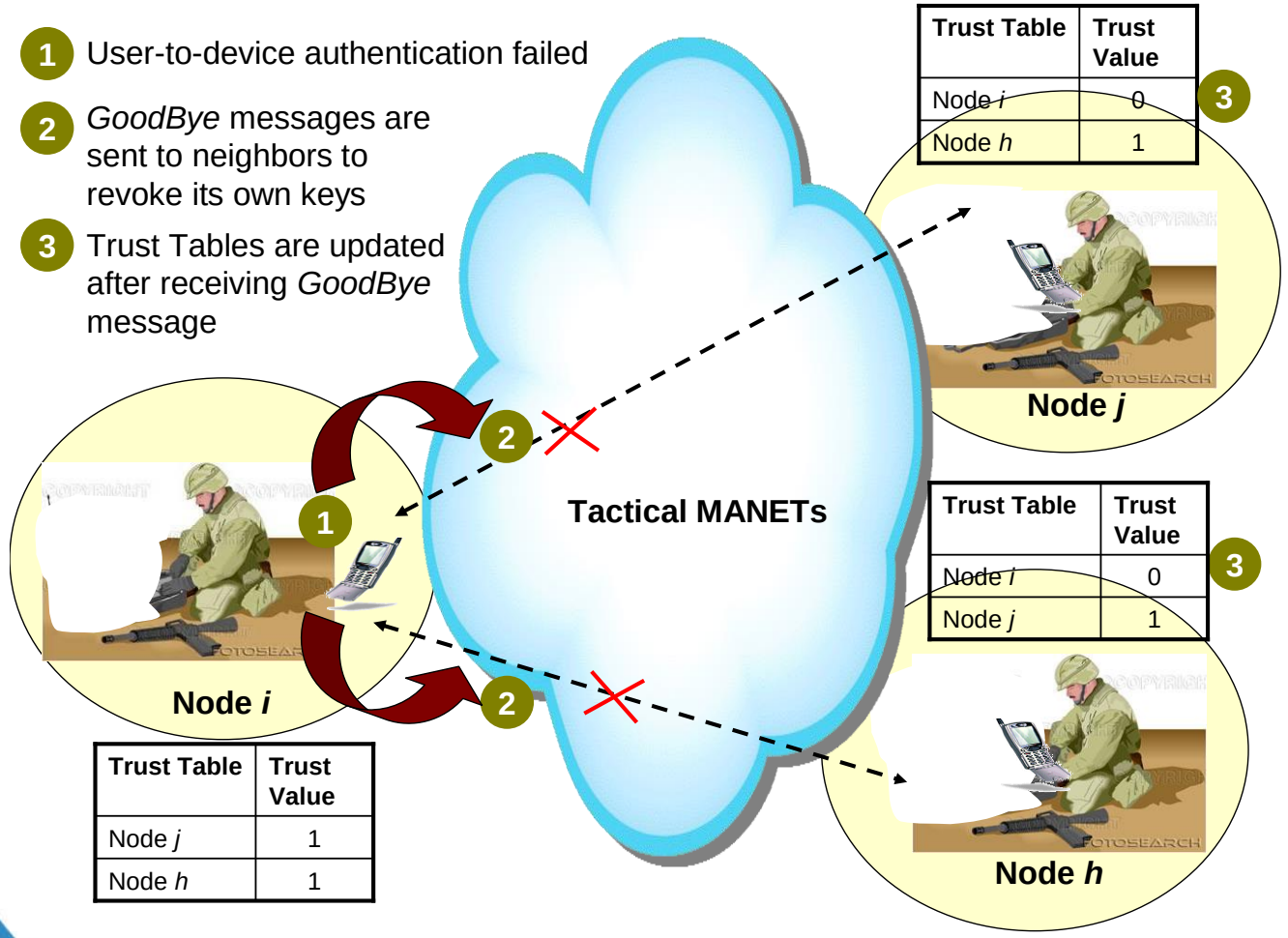
- For Intrusion Detection
  - Suspicious activity detected at one layer can lead to a response at another layer.
- For Frequency Hopping
  - The rate and range of frequency hopping can be tuned to current conditions and application level requirements
- For Distributed Authentication
  - The best nodes for authentication are chosen taking into account the current conditions (network and application) to minimise the overall threat posed to the network

Case Study: Overview of Lightweight Integrated Authentication

1. Bootstrapping
2. Pre-authentication
3. Credential establishment
4. Authentication
5. Monitoring
   - *Includes gathering and integrating trust values*
6. Revocation

Case Study: Self-Revocation in Lightweight Integrated Authentication

1. User-to-device authentication failed
2. *GoodBye* messages are sent to neighbors to revoke its own keys
3. Trust Tables are updated after receiving *GoodBye* message



Trust Table	Trust Value
Node *j*	1
Node *h*	1

Trust Table	Trust Value
Node *i*	0
Node *h*	1

Trust Table	Trust Value
Node *i*	0
Node *j*	1

Communications Research Centre (CRC)
Defence R&D Canada - Ottawa

Case Study: Cross Layering in Lightweight Integrated Authentication

- Session Layer
  - Sessions from un- or low-trusted nodes can be refused or dropped in times of high traffic
- Network Layer
  - Trusted routing can be created using input from other layers detecting mis-behaving nodes, ensuring only the most behaved nodes are used for forwarding sensitive packets
- MAC Layer
  - longer medium access time may be allocated to the nodes that have higher trust values
- Physical Layer
  - We can increase the trustworthiness of the spectrum sensing results by assigning higher weights to the sensing results obtained from nodes with higher trust values

Conclusions and Future Work

- There are many similarities between MANET and tactical networks that suggest similar security risks.
- This paper proposes the use of a cross-layer framework to help solve network security issues in tactical networks.
- We are currently in the process of designing a cross-layer intrusion detection service which makes use of the proposed framework.
  - We plan to use a simulation of tactical networks to gain quantitative measurements of the effectiveness of cross-layer controls compared to existing single layered controls.